VIRGINIA DEPARTMENT OF EDUCATION

Division of Technology

Designing and Optimizing

Ethernet Networks

January 2001

TABLE OF CONTENTS

1 Purpose and Overview

The purpose of this document is to provide guidelines to assist Virginia's schools and school divisions when installing new or upgrading existing networking infrastructure. Such guidelines enable schools to receive the greatest value from their technology investment by:

- Maximizing efficiency at each layer of the network.
- Improving reliability to minimize network outages.
- Minimizing staffing requirements.

The intent is to supplement the Preliminary Architectural Guidelines for the Web-based SOL Technology Initiative document.

Several general rules should be kept in mind as Virginia school divisions invest in the various network infrastructure components.

- Network infrastructures are constantly evolving. Therefore, networks must be modular to accommodate these changes. In addition, where possible, new technology components should be able to work within the current technical infrastructure and to grow with future computing demands.

- In moving forward, schools should consider networking technology that has been in use six to twelve months. Availability and support are far more important than having the absolute latest technology.

- Although both Ethernet and Token Ring networks are deployed in schools across the commonwealth, the predominant networking technology is Ethernet. This document focuses on guidelines for Ethernet networking. All new infrastructures should be Ethernet-based, not Token Ring.

- The key to network design is in understanding networking standards. Use a few standards, and use them across the entire network if possible. Optimizing the network starts by building the simplest network that will meet your needs; reaching consensus about network standards at the outset will save time and other resources.

Guidelines will be provided for the following areas:

- Local Area Networks
- Wide Area Networks
- Computing / Workstation Platforms
- Infrastructure Management

These guidelines are not to be interpreted as statewide standards.

2 Local Area Networks (LAN)

Local Area Networks are the data communications conduits within the confines of a school building or campus. LANs generally consist of devices (servers, workstations, etc.) that are connected together using hubs or switches. Routers are used to connect LANs, forming an enterprise environment.

Virtually every computer manufacturer supports Ethernet. This broad support, together with its low cost and flexibility are the major reasons for its popularity. Increased competition in the industry will continue to force a downward trend in prices while increasing the number of features and total system performance.

Most early LAN's were designed around the use of a shared communications channel. Recently, the following two developments occurred and fundamentally changed the way networks should be designed:

- The introduction of structured wiring standards has made creating a simple, reliable, and easy to manage cabling plant a reality.
- End user-computing equipment and application requirements have advanced to the point where the capacity of a shared LAN could actually limit overall performance.

These two factors, together with advances in technology have fostered the development and deployment of intelligent LAN switches. While traditional, shared-bandwidth hubs are still in use today; they are generally considered acceptable only at the edge of the network or to meet small workgroup requirements.

Switch - Short for port-switching hub, is a special type of hub that forwards packets to the appropriate port based on the packet's address. Conventional hubs simply rebroadcast every packet to every port. Since switching hubs forward each packet only to the required port, they provide much better performance. Most switching hubs also support load balancing and other technologies used to increase scalability and management.

The widespread acceptance of these devices brings another advantage - the abundance of management and troubleshooting tools. While these networks are stable and do not require daily maintenance, every network should include some provision for management. Most devices have management capabilities (Simple Network Management Protocol – SNMP) embedded in them and make it possible to administer the entire network from a central location.

2.1 Designing Local Area Network (LAN)

In designing a LAN infrastructure, it is important to optimize performance, especially user perception of performance, while minimizing costs. It should not be forgotten that the newest, fastest, most expensive equipment would not necessarily improve performance of services located on other networks. Optimizing the local area network begins by accessing your needs and environment.

2.1.1 Needs Assessment

In most cases, professional assistance may be required to perform a comprehensive assessment of the environment (e.g., using protocol analyzers or network sniffers). However, assistance isn't required to begin the process. Gathering information in advance will reduce the cost of any future assessment and help to identify potential bottlenecks. At a minimum, every assessment should:

- Document the names and types of new applications.
- Document the names and types of new protocols.
- Document the number of users requiring the new applications or protocols.
- Diagram the flow of information of existing applications.
- Diagram the flow of information when the new applications are introduced.
- Identify peak hours of usage of the new applications.

2.1.2 Network Design Models

Networks should be implemented using structured design models. Using these models, tasks are simplified by creating network in discrete layers (core, distribution, and access layers). These layers can be implemented in phases, as funding becomes available, which helps to control costs and provides an opportunity for training.

The Core Layer is the center of the network. It is used to provide the physical transfer of data between sites. This layer is critical to the success of every network installation, and as such, special care should be given when evaluating proposals for this layer. Essential elements to look for in this layer are:

- How efficient is it?
- Does it adapt to changes quickly?
- Does it provide sufficient redundancy and fault tolerance?

The Distribution Layer is the demarcation point between the Access and the Core layers of the network. This layer can have many roles, including implementing the following functions: policy, security, departmental or workgroup access and broadcast domain definition. Many smaller networks won't need to make use of this layer.

The Access Layer connects each individual device on a local segment to the network. Typically, these devices are characterized by the switches located in the wiring closets. VPN (virtual private network) and remote access or dial-up functions are located in this layer.

2.1.3 Network Services

The next step in designing a network is to select the protocols (e.g., TCP/IP, AppleTalk or IPX etc.) that are to be used within the network. Protocols define the set of rules that allow the various devices to communicate with each other across the entire network. In addition, other

services may be employed such as Domain Name Service (DNS) or Dynamic Host Configuration Protocol (DHCP), that automatically assign individual addresses.

Each protocol used requires a structured address scheme to provide proper communications. Along with this addressing scheme, developing a plan for assigning meaningful names to various network devices is essential to easing future maintenance tasks and speeding up the trouble-shooting processes.

Once implemented, this scheme would be difficult and costly to change. Therefore, schools are encouraged to consult with a professional network designer, if necessary, when making these determinations.

2.1.4 Protocol Selection

Since multiple protocols produce higher complexity and administration costs, it is best to use a single protocol in the environment. Since, it doesn't rely on broadcasts TCP/IP is more efficient than other protocols, and it is the most commonly used protocol available today.

2.1.5 TCP/IP Addressing

A well-planned TCP/IP address scheme allows for future growth of the network. School divisions may consider implementing Network Address Translation (NAT) on a proxy server or router to conserve IP addresses. The proxy server or router acts as a gateway which maps internal or private addresses to external or public addresses, as specified in RFC (Request for Comment) 1597.

Private IP address ranges are:

- 10.0.0.0 to 10.255.25.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

2.1.6 Network Security

Network Security is a wide-reaching topic -- and it can become extremely complex. Nevertheless, it is one aspect common to all environments, and it is crucial to the success of any environment. When thinking about security within the network, focus on the following areas (authentication, access control, and auditing). Each area requires its own technologies and techniques.

- Authentication: is used to prove the identity of the user
- Auditing: logging who performed various activities on the network
- Access Control: determining who should have access to various resources, and what level is required (e.g., read only, read & write etc.)

2.1.7 Other Services

Additional functions or services may be required to optimize network performance or increase services available to the users. While these are commonly found, they may not be needed in every case and should be evaluated on an individual basis. Additional services may include host access, file and printer sharing or remote access.

In providing these services, where possible, schools divisions should investigate using network appliances. A network appliance is self-contained device that provides limited or, in some cases, a single function. Their main advantages are they generally cost less and are easy to maintain. The services provided by these appliances range from Web caching solutions to e-mail, firewall, and Web servers.

3 Optimizing Your Network

Network Models:

This section provides a "rule of thumb" guide to enable a school division to make maximum use of its infrastructure based on four different models or classes of LAN likely to be found at various schools. Knowing which model a LAN most closely resembles will indicate where upgrades may be needed. This list is not complete, nor are the examples discrete. Each LAN may resemble more than one model.

These examples are based on the following criteria:

- Location of service(s), local or non-local
- Number of local services
- Distribution of users in relation to the local services
- Bandwidth needed by the services
- Number of network devices

Definitions:

Local versus non-local services:

Typically a local service will be in the same building as the user or can be accessed via a high-speed connection. Services located across a router or WAN link are considered non-local. An example of a local service would be a file server or database located on the same LAN as the user. A server located in the district office is an example of a non-local service.

Application Bandwidth requirements:

Low: Email, and character-based applications
Medium: Web browsing, File and Printer sharing and File transfers
High: Some applications, non-client server databases, and CAD workstations

Number of devices per segment:

Low: up to 25 devices
Medium: 26-100
High: 100+

Speed of Connection:

Low: Shared 10Mbps
Medium: Switched 100Mbps Full Duplex
High: Switched 100Mbps Full Duplex or faster (e.g., Fast Ethernet or Gigabit Ethernet)

Example Scenarios

1) Non-local service(s)

In this scenario, all the client workstations access a non-local service or services. In most cases, the bottleneck is likely to be the WAN connection.

To improve WAN performance, use SLA (Service Level Agreements) and verify that the service provider is meeting requirements. Other options include: increasing the size of the WAN connection or installing a second WAN link and routing a portion of users across each connection. To improve Internet browsing, consider installing a Web-caching device.

2) One or few local services used by all LAN clients

In this scenario, all clients access one or more local services. Depending upon both the service requirements and the number of networked devices, local bandwidth may be managed by using switched 10/100 media.

Verify that the application servers and other network resources are using high bandwidth connections (e.g. 100Mbps switched full duplex). Another option would be to install a second network card in the servers and configure network load balancing. Prior to implementing this, verify that the servers have capacity to handle the additional traffic.

3) Multiple local services used by respective subsets of clients

This situation can be referred to as a workgroup-based LAN. Few or none of the clients requires access to all local services. Rather they tend to be discrete groups of clients, each using a different service.

In this scenario, all clients access one or more local services. In this case, LAN performance can be improved by implementing switched 10/100 media. Verify that the application servers and other network resources are using high bandwidth connections (e.g. 100Mbps switched full duplex). An additional option would be to install second network card in the servers and configure network load balancing. Also, consider placing the individual resources in proximity with its prospective pool of users. A VLAN (virtual LAN) could be used to further segment broadcast traffic.

4) Several clusters of high bandwidth services

In this scenario, several or more servers are accessed by users across the environment. All servers require high bandwidth connections to properly service the user community.

Eliminating hardware constraints in each device in this scenario is imperative. At a minimum, each server should use a switched 100Mbps with load balancing for redundancy or aggregate channels to create a faster connection. Consider moving the majority of servers to a central location within a high-speed server “farm”.

Install switches in each closet, using a gigabit uplink back to the main wiring closet. To further segment the traffic, consider using additional technologies such as Layer 3 switching and VLANs.

Recommendations for optimizing LAN connectivity:

- Start building the network from the core layer out.
- Remove token ring and migrate to an Ethernet topology.
- Standardize on a single protocol suite, preferably TCP/IP.
- Define a scheme for naming and assigning addresses to each device on the network. Names should follow geographical boundaries or function; IP addresses should be private (i.e., not available on the Internet).
- Replace shared hubs with 10/100 Ethernet switches. At a minimum, NIC (network interface card) drivers may need to be upgraded or, in some cases replaced, to take advantage of the new switches.
- Implement network load balancing on critical servers. Be sure that servers have the hardware capacity to support additional throughput.
- Do not use network servers and other software applications to route traffic. Use routers, switches or enhanced firewalls to segment and route network traffic..
- To improve name resolution and manageability, implement DNS (Domain Name Service). Installing DNS locally will reduce the traffic on the WAN links. Consider using DHCP (dynamically assigned IP addresses).
- Create a mechanism for managing the network and capture performance statistics (e.g., bandwidth utilization, number of collisions and server utilization etc.). Use this information to create a baseline of the networks' performance and forecast future requirements.
- Ethernet networks should be segmented if network utilization is above 40 percent for an extended period.
- Where possible, use network hardware made by a single vendor. Over time this will create a more consistent environment and may reduce overall costs.
- Document the network infrastructure (e.g., wiring closets, cable runs etc.) using a set of blueprints.

4 Wide Area Network (WAN)

Wide Area Networks are the real time data communication conduits between district buildings or other resources. WANs are generally comprised of routers, switches, and communications circuits provided by telecommunications companies or other Internet Service Providers (ISP). The speed or bandwidths of these connections include 64Kbps, 128Kbps – 1.544Mbps (Fractional T1 – Full T1), 45Mbps (DS3) and up to 155Mbps (OC3).

When the school division provides the Internet connection to its schools, care must to taken not to over allocate that connection. In other words, regardless of the speed at which the district is connected to the Internet, divide that speed equally among the schools ultimately serviced by that connection.

Example:

> School division has a single T1 (1.544Mbps) connection to the Internet and there are eight schools each with a 256Kbps connection to the district office. Effectively, each school has only 128Kbps connection to the Internet.

There are a few ways to address the bandwidth constraint issue. Other than adding additional bandwidth, consider installing a Web-caching device to improve Internet performance. These devices should be installed as close as possible to its users. Some of the advances in technology (i.e., QoS – Quality of Service or CoS – Class of Service) provide a means of reserving or partitioning bandwidth. Schools are encouraged to consult with a professional network designer to obtain the latest information on these tools.

Recommendations for optimizing WAN connectivity:

- When the school division provides the Internet connection to its schools, care must be taken not to over allocate or saturate that connection.
- To locate an ISP, contact the district office, the local Telephone Company, or use www.getspeed.com.
- Do not use network servers and other software applications to route traffic. Use routers, switches or enhanced firewalls to segment and route network traffic.
- Offload non-essential tasks from the router.
- Routing protocols determine what information is exchanged between routers across WAN links. Some protocols are more efficient than others. Work with your ISP or hardware vendor to determine what works best in your environment.
- Each network needs to be protected from the public Internet using a firewall or other technology. Preferably, some combination of these options could be used.

5 Computing / Workstation Platforms

Computing Platforms consist of hardware platform (e.g., PC or Macintosh), the software operating system (OS), and utility services (anti–virus, tape backup, disk maintenance, etc.) for both servers and clients. The Network Operating System (NOS), which is the server OS, is also included in this section.

School divisions should purchase widely available computing platforms with the most powerful components they can afford to increase the useful life of the device. The industry is evaluating thin clients and Business PCs as a complement to high-end computing platforms.

Hardware for both servers and workstations should be procured from major providers or their designated representatives. These providers use commercial-grade components with lower failure rates, but more importantly, they provide greater consistency in product offerings. Over time, a consistent product base will significantly reduce administration and support.

Contracted maintenance services are also more readily available for major manufacturer's products. Consider the extended on-site warranty options when selecting a vendor or vendors

School divisions should consider the work of the Southern Regional Education Board (SREB) in its report, *Guidelines for Technology Equipment and Use: An SREB Model for Schools and Campuses*.

Recommendations for computing / workstation platforms:

- Remove unneeded protocols and services from workstations and servers.
- Update essential software applications and device drivers (e.g., virus scanners, network card software and operating system patches etc.).
- Monitor server performance on a regular basis. Create a baseline and use it to forecast future requirements.
- Develop a means to identify and backup critical applications and servers.

6 Infrastructure Management

Effective management is critical for minimizing the administrative burden of the network and for maximizing its reliability and performance. The end users, policy, procedures, tools, information systems personnel, and training must work together to manage the overall infrastructure. To utilize this resource effectively, budgets should reflect the ongoing cost of investments in technology.

Recommendations for Infrastructure Management:

- Total cost of ownership (TCO) projections should be considered in the budget as well as start-up costs.
- Appropriate staffing should be deployed for administration of the servers and network.
- Technology support positions should be dedicated to the operation and maintenance of the resource. Unique strategies should be developed to recruit and retain qualified information technology staff.
- Workstations should be replaced on a regular basis. School divisions should plan for a three to five-year life.
- Leasing and seat management options could possibly be evaluated as an alternative to buying equipment. Leasing would provide a method to regularly update equipment.
- Infrastructure management tools to configure, monitor, troubleshoot, and report on the environment should be available. Basic configuration and monitoring tools from the manufacturer should be supplemented with other applications and utilities as required.
- Outsourcing specific tasks (e.g., stocking of spare parts or break/fix maintenance) is generally advantageous and should be explored. Each task should be evaluated for overall cost.
- Security policy should detail the establishing and removing user accounts, gaining secure access, and procedure for dealing with violations.
- Acceptable use policies should be in place and enforced. These should be reviewed and updated periodically.

Total Cost of Ownership as it relates specifically to schools and school divisions is discussed in the publication entitled *Taking TCO to the Classroom: A School Administrator's Guide to Planning for the Total Cost of New Technology* developed by the Consortium for School Networking (CoSN).

7 References

Spurgeon, Charles E., Ethernet: The Definitive Guide, O'Reilly & Associates, Inc., 2000 (ISBN: 1-56592-660-9). Charles Spurgeon's, Ethernet Web Site can be found at the following URL (http://www.ots.utexas.edu/ethernet)

Seifert, Rich, The Switch Book, John Wiley and Sons, Inc., 2000

The Tolly Group web site contains extensive testing and other product information regarding many types of network components. URL (http://www.tolly.com)

RFC 1597: Address Allocation for Private Internets, this document can be found on the web at URL (http://www.pku.edu.cn/academic/research/computer-center/tc/html/RFC1597.html).

Telecommunications Industry Association (TIA) and the Electronic Industries Association (EAI), *TIA/EIA-568-A Commercial Building Telecommunications Cabling Standard*. This standard specifies a cable plant which is application generic, in that it is suitable for most voice, video, and data applications.

Southern Regional Education Board (SREB), *Guidelines for Technology Equipment and Use: An SREB Model for Schools and Campuses.* This SREB report is available at URL (http://www.sreb.org/programs/EdTech/pubs/techselectguidelines/EdTechGuidelines.pdf).

Consortium for School Networking (CoSN),*Taking TCO to the Classroom: A School Administrator's Guide to Planning for the Total Cost of New Technology.* This report is available at URL (http://www.cosn.org/tco/tco2class.pdf).